REMARKS

In response to the Advisory Action mailed March 12, 2008, Applicant respectfully requests reconsideration. To further the prosecution of this Application, Applicant submits the following remarks and has cancelled claims. The claims as now presented are believed to be in allowable condition.

Claims 1, 2, 4-20, 31, 38-41, and 43-51 were pending in this Application. By this Amendment, claim 43 has been canceled. Independent claim 1 has been amended to include substantially the content of cancelled dependent claim 43. Additionally, each of independent claims 38 and 47 has been amended to include substantially the content of claim 43. The amendments do not add new matter to the Application. Accordingly, claims 1, 2, 4-20, 31, 38-41 and 44-51 are now pending in this Application. Claims 1, 38, and 47 are independent claims.

Rejections under §102 and §103

Claims 1-2, 4-7, 9-11, 14-18, 31, 38-41, and 43-51 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,623,637 to Jones (hereinafter Jones) in view of the article by Spelman, et al., U.S. Patent No. 5,638,445 (hereinafter Spelman). Claim 8 was rejected under 35 U.S.C. §103(a) as being unpatentable over Jones and Spelman as applied in claim 1 and further in view of the article by Schneier, Bruce, entitled Applied Cryptography: Protocols, Algorithms, and Source Code in C, pp. 383-387, 600, New York: John Wiley & Sons, Inc., 1994 (hereinafter Schneier). Claims 12-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones and Spelman as applied in claim 1 and further in view of U.S. Patent No. 5,922,074 to Richard, et al. (hereinafter Richard). Claims 19-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones and Spelman as applied to claim 43 and further in view of U.S. Patent No. 6,505,164 to Brunsting, et al. (hereinafter Brunsting).

Applicant respectfully traverses the rejections of claim 11, 38, and 47 as amended and requests reconsideration. The claims are in allowable condition.

Each of independent claims 1, 38, and 47 has been amended to include substantially the content of claim 43. Taking claim 1 as an example, claim 1 relates to a method that includes implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret. The method includes authenticating the client by a device, the device storing an encrypted secret and configured not to provide the encrypted secret without authentication. The method includes after authenticating, providing to the client by the device the encrypted secret, wherein the encrypted secret is capable of being decrypted using a decryption key derived from the third secret and wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret. Implementing the multi-party secure computation protocol involves at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server. Implementing the multi-party secure computation protocol also involves at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client and at the client, deriving the third secret from the intermediate data.

While independent claims 1, 38, and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view of Spelman, independent claims 1, 38, and 47 as amended are patentable over Jones in view of Spelman

because neither Jones nor Spelman teaches or suggests all of the elements of independent claims 1, 38, and 47 as amended. For example, neither Jones nor Spelman teaches or suggests a multi-party secure computation protocol comprising "at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server, at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client, and at the client, deriving the third secret from the intermediate data," as claimed by the Applicants.

Jones relates to methods and apparatus for storing, processing, and communicating private data. Column 1, lines 11-12. In the rejection of independent claims 1, 38, and 47 the Final Office Action recites on page 4 that "Jones does not disclose a protocol wherein the client has a client secret and the server has a server secret used to compute a third secret from the client and server secret and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret." Accordingly, Jones does not teach or suggest "at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server, at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client, and at the client, deriving the third secret from the intermediate data," as claimed by the Applicants.

Spelman does not cure the deficiencies of Jones. The Final Office Action on page 4 recites "Spelman teaches a method for blind encryption (title). Spelman [teaches] a protocol wherein the client (merchant) has a client secret (GSO) and the server (merchant acquirer) has a server secret (PI) used to compute a third secret $C[GSO]_{k1}$, $D[PI]_{k2}$, $E[k1 \ldots]_R$, and $E[k2 \ldots]_R$ from the client

and server secret, wherein the protocol is implemented so that the client obtains the third secret…"

With such a recitation, the Office Action equates the merchant 20 of Spelman with the client as claimed by the Applicants, equates the merchant acquirer 40 of Spelman with the server as claimed by the Applicants, and equates the four pieces of encrypted data from the consumer 10, namely $C[GSO]_{k1}$, $D[PI]_{k2}$, $E[k1\ Merchant\ name]_R$, and $E[k2\ credit\ card\ number]_R$, with the third secret of the Applicants claims. However, based upon such an recitation, Spelman does not teach or suggest implementing a multi-party secure computation protocol comprising "at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server, at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client, and at the client, deriving the third secret from the intermediate data," as claimed by the Applicants.

Spelman relates public-key cryptography and key distribution. Column 1, lines 5-6. In Spelman, a protocol involves four participants: a consumer 10, a merchant 20, a recryptor 30, and a merchant acquirer 40 (e.g. a bank). Column 4, lines 24-27. In Spelman, in the case where the consumer 10 wishes to purchase certain goods and/or services from the merchant 20, the consumer 10 generates four pieces of encrypted data for the merchant 20: an encrypted goods and services order (GSO), symbolized $C[GSO]_{k1}$, an encrypted purchase instruction (PI), symbolized $D[PI]_{k2}$, a GSO key exchange blob, symbolized $E[k1\ Merchant\ name]_R$, and a PI key exchange blob, symbolized $E[k2\ credit\ card\ number]_R$ and sends the four pieces of information to the merchant 20. Column 5, lines 16-65.

In Spelman, the merchant 20 receives an encrypted GSO, symbolized $C[GSO]_{k1}$, an encrypted PI, symbolized $D[PI]_{k2}$, a GSO key exchange blob, symbolized $E[k1\ Merchant\ name]_R$, and a PI key exchange blob, symbolized $E[k2\ credit\ card\ number]_R$ from the consumer 10 (i.e., the Applicants' third secret as asserted by the Office Action). The merchant 20 then sends only the two key exchange blobs to the recryptor 30 and receives two new key exchange blobs from the recryptor 30. The merchant 20 then sends to the merchant acquirer 40 the block encrypted PI (i.e., $D[PI]_{k2}$) and the re-encrypted PI key exchange blob, $E[k2\ credit\ card\ number]_A$..

Spelman does not teach or suggest implementing a multi-party secure computation protocol comprising "at the client, deriving the third secret from the intermediate data," as claimed by the Applicants. As indicated in Spelman, the ***consumer 10*** generates $C[GSO]_{k1}$, $D[PI]_{k2}$, $E[k1\ Merchant\ name]_R$, and $E[k2\ credit\ card\ number]_R$ (e.g., the Applicants' third secret as asserted by the Office Action). There is no teaching or suggestion that the merchant 20 of Spelman (i.e., the Applicants' client as asserted by the Office Action) as "deriving the third secret from the intermediate data," as claimed by the Applicants. Instead, Spelman describes the merchant 20 as ***receiving*** the encrypted data $C[GSO]_{k1}$, $D[PI]_{k2}$, $E[k1\ Merchant\ name]_R$, and $E[k2\ credit\ card\ number]_R$ (e.g., the Applicants' third secret as asserted by the Office Action) from the consumer 10.

For the reasons stated above, claims 1, 38, and 47 as amended patentably distinguishes over the cited prior art, and the rejection of claims 1, 38, and 47 under 35 U.S.C. §103(a) should be withdrawn. Accordingly, claims 1, 38, and 47 are in allowable condition. Furthermore, because claims 2, 4-20, 31, 44-46, and 49 depend from and further limit claim 1, because claims 39-41, 48, and 50 depend from and further limit claim 38, and because claim 51 depends from and further limits claim 47, claims 2, 4-20, 31, 39-41, 44-46, and 48-51 are in allowable condition for at least the same reasons.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Jeffrey J. Duquette/

Jeffrey J. Duquette, Esq.
Attorney for Applicant
Registration No.: 45,487
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1048-006

Dated: April 14, 2008